

DETD(146)

Accordingly, . . . decrypt the communications of the wiretapped user. If the warrant (and any applicable grace period) has expired, the wiretapped user's **private key** is **erased** and will not be recreated again under that warrant by the decoder box (unless a new warrant having a new. . . .

DETDESC:

DETD(228)

In . . . decryption key, and as a result receives an escrow certificate for the corresponding new public encryption key, the device will **erase** the previous **private key** in order to force reliance of the device on the newly escrowed **private key**. Alternatively, the device could retain the previous **private key** for only a short time as needed, e.g. for the time needed to recover data encrypted into data storage using. . . apply to its domestic escrow agents who can verify the owner's certificate already in their possession and release the actual **private key** splits. This procedure relieves the device owner of any extra legal formalities that might be required in order to obtain. . . .

=> d his

(FILE 'USPAT' ENTERED AT 09:56:10 ON 09 DEC 1998)
L1 (88931)S FOOD
L2 615 S PRIVATE KEY
L3 0 S DELETE?(W)PRIVATE KEY
L4 83549 S DELETE? OR REMOVE?(W)PRIVATE KEY
L5 78 S (DELETE? OR REMOVE?)(2P)PRIVATE KEY
L6 101 S (DELETE? OR REMOVE? OR ERASE?)(2P)PRIVATE KEY

=> s 16 and public key

59744 PUBLIC
162482 KEY
958 PUBLIC KEY
(PUBLIC(W)KEY)
L7 86 L6 AND PUBLIC KEY

=> s 17 and certificat?

5672 CERTIFICAT?